Security Improvement of a Transformed-key Asymmetric Watermarking System

F. Benedetto[1], G. Giunta[2]

Signal Processing for Telecommunications and Economics Lab., University of Roma Tre,
via della Vasca Navale 84, 00146 Rome, Italy

[1]francesco.benedetto@uniroma3.it; [2]gaetano.giunta@uniroma3.it

Abstract

An effective asymmetric watermarking procedure has been recently devised in literature, named Transformed-key Asymmetric Watermarking (TKAW). A weakness point of this system is its vulnerability against projection attacks, as well shown by Chen and Ye. This work discusses a modified version of the TKAW to provide robustness against projection attacks, by means of a non-linear transformation, without increasing the computational complexity of the original method but with the same performances.

Keywords

Authentication; Digital Watermarking; Asymmetric Watermarking; Attacks and Countermeasures

Introduction

Digital watermarking of multimedia contents has become a very active research area over the last several years (*Fu, 2012; Benedetto and Giunta, 2011; Bonuccelli et al., 2007; Li and Hung, 2011*). In a networked environment like the World Wide Web, the crucial issue to be satisfied is the necessity to answer the ever-growing need to protect the intellectual property (copyright) of digital still images, video sequences, and audio from piracy attacks, maintain a high Quality of Service (QoS) of the communication link (*Ahmed et al., 2006; Benedetto et al., 2009, Campisi et al., 2002*). The aim of a controlled distribution of multimedia data can be reached developing suited signal processing techniques, such as digital watermarking (*Benedetto et al., 2007; Benedetto et al., 2005; Zang and Zhou, 2010*). Although copyright protection was the very first application of watermarking, different uses have been recently proposed in the literature (*Benedetto et al., 2012b*). Fingerprinting, broadcast monitoring, data authentication, multimedia indexing, content-based retrieval applications are only a few of the new applications where watermarking can be usefully employed (*Boato et al., 2008; Benedetto et al., 2011*). Most of these watermarking schemes are symmetric watermarking procedures meaning that the same key is used for watermark embedding and extraction, allowing piracy attacks when the watermark is known by a third party and can be easily removed (*Ahmed and Syial, 2005; Xie et al., 2007*). As a consequence, new schemes of asymmetric watermarking have been recently proposed in literature (see for example: *Boato et al., 2008; Boato et al., 2007; Boato et al., 2006; Mi He and Lizhi Cheng, 2008; Jun et al., 2007; Jun and Jun, 2009; Gui and Chen, 2006a; Gui and Chen, 2006b; Furon and Duhamel, 2003; Tzeng et al., 2005*). In particular, an asymmetric watermarking procedure has been devised by (*Choi et al.*, 2004) named transformed-key asymmetric watermarking (TKAW) system, in which two different keys are used for watermark embedding (i.e. encoding) and extraction (i.e. decoding), respectively. The TKAW scheme renders asymmetry through a transform matrix (i.e. a linear transformation). The asymmetric watermarking procedure proposed by (*Choi et al.*, 2004) is really effective but has a great weakness point, as it was demonstrated by (*Chen and Ye, 2006*): in fact, the TKAW scheme is really vulnerable to projection attack. (*Chen and Ye, 2006*) show that for the TKAW system the inner product of the received signal and public key almost equals to zero and, as a result, it cannot resist projection attack.

In this work, we propose a modified version of the TKAW procedure in order to provide robustness against projection attacks, by means of a non-linear transformation, without increasing the computational complexity of the original method and with the same performances. The remainder of this work is organized as follows. In Section II, we describe the modified TKAW scheme by means of a non-linear transformation, showing that this new procedure maintains the same system performance of the original method. Section III is about the security analysis of the

new scheme showing its robustness against the projection attack while Section IV briefly concludes the work.

Modified TKAW System

In the original TKAW system, (*Choi et al.*, 2004), the asymmetry is realized through a transformation matrix A. In particular, let u_i be a set of orthonormal sequences with i = 1, …, k then the coding and decoding keys, $w_{s,i}$ and $w_{s,j}$ respectively, are obtained as follows:

$$w_{s,i} = \frac{Au_i}{\|Au_i\|} = \gamma_s Au_i ,$$

$$w_{p,i} = \frac{A^{-t}u_i}{\|A^{-t}u_i\|} = \gamma_p A^{-t}u_i \quad (1)$$

with $\gamma_s = \|Au_i\|^{-1}$, $\gamma_p = \|A^{-t}u_i\|^{-1}$ and where A is an n x n matrix and A^{-t} denotes inverse transpose. The embedding process is then realized by means of the rule $y = x + \alpha \cdot w_{s,i} = x + \alpha \cdot \gamma_s \cdot A \cdot u_i$, where x is the host signal and α, the power of the mark, is a scaling factor that determines the watermark strength and is adjusted to a value that makes the watermark imperceptible.

The decoding (i.e. watermark detection) process is a usual correlation process between the decoder input r and the decoding key $w_{p,j}$ (i.e. public detection). In particular, the decoder evaluates the inner product between r and $w_{p,j}$ as follows:

$$C_j = w_{p,j}^t r = \gamma_p u_j^t A^{-t}\hat{x} + \gamma_p u_j^t A^{-1}\alpha\gamma_s Au_i = \\ = \gamma_p u_j^t A^{-1}\hat{x} + \alpha\gamma_p\gamma_s u_j^t u_i \quad (2)$$

Then, by comparing C_j with the threshold $T = \left(E[C_i] + 2E[C_j]\right)/3$, the watermark can be detected, where obviously $E[\cdot]$ denotes the expectation operator. Choi et al designed the system so that $u_j^t A^{-1}\hat{x} \approx 0$ and $C_j \approx \alpha\gamma_p\gamma_s u_j^t u$. The TKAW system is an efficient asymmetric watermarking system but, as we can see, it is based on a linear transformation by means of the transformation matrix A. Moreover, the TKAW also needs $u_j^t A^{-1}\hat{x} \approx 0$, which means it can be defeated by a standard projection attack as well shown in (*Chen and Ye, 2006*).

We propose here a new modified version of this algorithm in which the asymmetry is given by a non-linear transformation, allowing the same system performance and more robustness against the projection attack. More in details, following the same mathematical approach of (*Choi et al.*, 2004), we modify the encryption and decryption keys, respectively, as follows:

$$w_{s,i} = \frac{e^{Au_i}}{\|e^{Au_i}\|} = \gamma_s e^{Au_i} ,$$

$$w_{p,i} = \frac{e^{A^{-t}u_i}}{\|e^{A^{-t}u_i}\|} = \gamma_p e^{A^{-t}u_i} \quad (3)$$

where the asymmetry is now given by means of an exponential of the matrix A (non-linear transformation). To compare the modified version with the original TKAW, we employ a watermark insertion in the wavelet transform domain. As in (*Choi et al.*, 2004), we consider images of size 512 x 512, octave-band decomposed into seven sub-bands in two levels using Daubechies filters, and the private watermark is added in the three mid-frequency sub-bands. Fig. 1 shows here the visual comparison between the *Lena* image watermarked with the original TKAW system (PSNR = 42.6 dB) and with the modified algorithm (PSNR = 40.86 dB): we obtain a negligible difference of less than 4% on the PSNR. Then, we have matched in our simulation results the performance of the original TKAW system obtaining the same performance, in terms of robustness against public attacks, as shown in details in the following.

In particular, regarding the analysis about public attacks, we consider as in (*Choi et al.*, 2004) that an attacker tries to confuse the public detector by subtracting a properly scaled public key $\beta \cdot w_{p,i}$ obtaining $\hat{y} = \hat{x} + \alpha \cdot w_{s,i} - \beta \cdot w_{p,i}$ where β is a constant value. The detector's output becomes $C_i = w_{p,i}^t \hat{y}$. Now, considering $w_{p,j}^t w_{s,i} = \gamma_s\gamma_p \left(A^{-t}u_j\right)^t \left(Au_i\right) = \rho\delta_{ij}$ where δ_{ij} is the Kronecker Delta and ρ is the correlation coefficient between $w_{s,i}$ and $w_{p,j}$, and denoting the cross-

correlation values among the two watermarks by ε_s and ε_p respectively, we can now re-write the detector's output as:

a)

b)

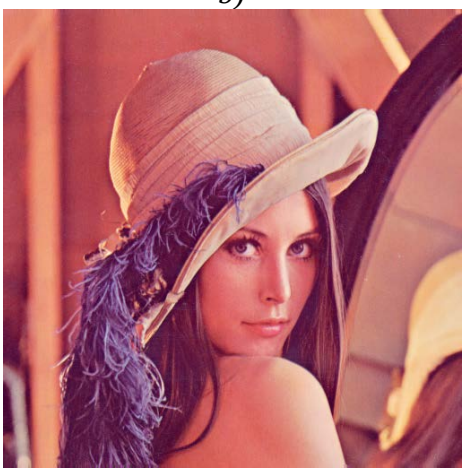

FIG. 1 *LENA* IMAGE: ***A)*** ORIGINAL TKAW WATERMARKED; ***B)*** MODIFIED TKAW WATERMARKED

$$C_j = \begin{cases} \approx \alpha\rho - \beta & if \quad j = i \\ \approx -\beta \in_p & if \quad j \neq i \end{cases} \tag{4}$$

assuming the correlation between the host signal and the watermark sufficiently small, as in (*Choi et al.*, 2004). The influence of this attack can be described in terms of the parameter β, which is 0 if there is no public attack. The merit of the original TKAW system, which holds on also in its modified version, in relation to the attacks is in that watermark detection by private key is still possible when the public detection is disabled. As done before with the public key, the correlation output in the detection using the private key is as follows:

$$C_j = \begin{cases} w_{s,j}^t \hat{y} \approx \alpha - \beta\rho & if \quad j = i \\ w_{s,j}^t \hat{y} \approx \alpha \in_s & if \quad j \neq i \end{cases} \tag{5}$$

Obviously, the two (public and private) keys must obey to the same requirements of the original algorithm in order to perform the same effectiveness and robustness. In particular, the matrix A must be chosen in order to have the correlation coefficient ρ=0.5, as well depicted in (*Choi et al.*, 2004). This requirement is of fundamental importance because attackers cannot disable both the public detection and the private detection at the same time. This feature provides additional security to the modified TKAW system. This is illustrated in Fig. 2 where we have obtained the same results of the Fig. 1 published in (*Choi et al.*, 2004), showing that the modified TKAW system holds the same performance as the original approach, versus different values of the parameter $\varnothing$. In the following Section, we describe how the modified TKAW system can outperform the projection attack.

Security Analysis about Projection Attack

One of the weakness points of the original algorithm TKAW is its vulnerability against projection attacks as well discussed by (*Chen and Ye, 2006*), since the asymmetry of the TKAW system is realized by means of a linear transformation. (*Chen and Ye, 2006*) discuss how to find the closest un-watermarked $\tilde{y}$ to the watermark-embedded signal y and they also show that the difference between y and $\tilde{y}$ is less than the watermark energy α. Therefore, the TKAW system cannot resist projection attacks. Here, we explain that using the modified TKAW system, the difference between y and $\tilde{y}$ is greater than the power of the mark, α, and therefore the algorithm is robust against projection attacks In particular, following the same methodological approach of (*Chen and Ye, 2006*), we denote with $r = y + n$ the received signal (which is the watermark-embedded signal y combined with an additive noise n) and with $\tilde{y} = r + tw_{p,j}$ the un-watermarked signal, i.e. the projection of y in the same hyperplane on which $\hat{x}$ falls, (*Chen and Ye, 2006*). As well depicted by (*Chen and Ye, 2006*), the original TKAW system must satisfy the following condition:

$$\left\langle w_{p,j}, \hat{x} \right\rangle = 0 \tag{6}$$

thus, with a projection attack we have $\langle w_{p,j}, \tilde{y} \rangle = (w_{p,j})^T (r + t w_{p,j}) = (w_{p,j})^T r + t \|w_{p,j}\|^2 = 0$, finally obtaining:

$$\tilde{y} = r - \frac{(w_{p,j})^T r}{\|w_{p,j}\|^2} w_{p,j} \quad (7)$$

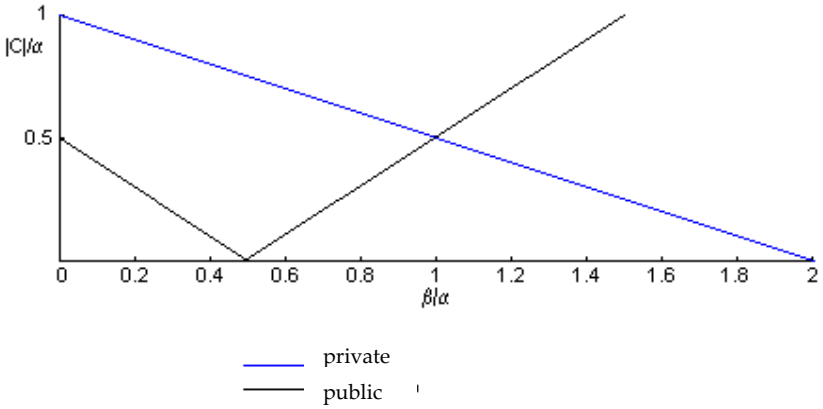

FIG. 2 PRIVATE AND PUBLIC DETECTION AGAINST PUBLIC ATTACK WITH CORRELATION COEFFICIENT $\rho = 0.5$

that is the closest solution against watermark-embedded signal. Moreover, (*Chen and Ye, 2006*) illustrated that the difference between y and $\tilde{y}$ is less than the watermark energy α:

$$\|y - \tilde{y}\| \leq \|y - x\| = \|\alpha w_{s,i}\| = |\alpha| \quad (8)$$

In particular, with the original TKAW system the difference in (8) equals the power of the watermark and the system cannot resist projection attack. This is not more valid using the modified version of the TKAW system we propose. In fact, since the asymmetry is now given by means of a non-linear transformation, the difference between y and $\tilde{y}$ is greater than the parameter α. In particular, with our modified algorithm we obtain the following value $\|y - \tilde{y}\| = 9$ with α = 0.1. Therefore, we can conclude that:

$$\|y - \tilde{y}\| > |\alpha| \quad (9)$$

This means that the obtained un-watermarked image is really different from the watermarked one, i.e. the modified TKAW system can now resist projection attacks.

Conclusions

This work has devised a modified version of the TKAW procedure in order to provide robustness against projection attacks, by means of a non-linear transformation. We have matched the performance of the original TKAW system obtaining the same robustness against public attacks. In particular, the merit of the original TKAW system, which holds on also in its modified version, is represented by the fact that watermark detection by private key is still possible when the public detection is disabled.

On the other hand, one of the weakness points of the original TKAW was its vulnerability against projection attacks, since the asymmetry was realized by means of a linear transformation. Here, we have shown that the modified TKAW system can now resist projection attacks. In fact, since the asymmetry is now given by means of a non-linear transformation, the difference between the watermarked signal y and its closest un-watermarked copy is greater than the watermark energy α.

REFERENCES

Ahmed, F., Sattar, F., Siyal, MY, Yu, D., "A Secure Watermarking Scheme for Buyer-Seller Identification and Copyright Protection", EURASIP Journal on Applied Signal Processing, Volume.2006, pp.1, 2006.

Ahmed, F., Siyal, MY, "A Hybrid- Watermarking Scheme for Asymmetric and Symmetric Watermark Extraction", 9th IEEE INMIC International Multitopic Conference, pp. 1 – 6, 2005.

Benedetto, F., Giunta, G., "An Effective Code Generator for Frequent Authentication of Multimedia Contents in

Mobile Applications and Services", 73rd IEEE Vehicular Technology Conference (VTC Spring), pp. 1 – 5, 2011.

Benedetto, F., Riganti Fulginei, F., Laudani, A., Albanese, G., "Automatic Aircarft Target Recognition by ISAR Image Processing based on Neural Classifier", International Journal of Advanced Computer Science and Application (IJACSA) , vol. 3, no. 8, pp.96-103, 2012.

Benedetto, F., Giunta, G., Neri, A., "A Bayesian Business Model for Video-Call Billing for End-to-End QoS Provision", IEEE Trans. on Vehicular Technology , vol. 58, no. 2, pp. 836 - 842, Feb. 2009.

Benedetto, F., Giunta, G., Neri, A., "QoS Assessment of 3G Video-Phone Calls by Tracing Watermarking Exploiting the New Colour Space "YST"", IET Communications (formerly IEE Proceedings on Communications), vol. 1, no. 4, pp. 696 - 704, Aug. 2007.

Benedetto, F., Giunta, G., Neri, A., "A new color space domain for digital watermarking in multimedia applications", IEEE int. conference Image Processing, ICIP 2005, Genova (Italia), 2005.

Benedetto, F., Giunta, G. Tedeschi, A., "Performance Analyis of Tracing Watermarking in the YST Domain for 3G Video-on-Demand Applications" - International Journal of Sensor Networks and Data Communications, vol. 1, 7 pages, 2012. DOI: 10.4303/ijsndc/X110504

Boato, G., De Natale, F.G.B., Fontanari, C., "A Multilevel Asymmetric Scheme for Digital Fingerprinting", IEEE Transactions on Multimedia, Volume.10, Issue.5, pp.758, 2008, ISSN: 15209210,

Boato, G., Conci, N., Conotter, V., De Natale, F.G.B., Fontanari, C., "Multimedia asymmetric watermarking and encryption", Electronics Letters, vol. 44, no. 9, pp. 601-602, Apr. 2008.

Boato, G., De Natale, F.G.B., Fontanari, C., Perez-Gonzalez, F., "Statistical Analysis of a Linear Algebra Asymmetric watermarking Scheme", Image Processing, 2007. ICIP 2007. IEEE International Conference on, On page(s): V - 485 - V - 488 Volume: 5, Sept. 16 2007-Oct. 19 2007.

Boato, G., De Natale, F.G.B., Fontanari, "An Improved Asymmetric Watermarking Scheme Suitable for Copy Protection", IEEE Trans. on Signal Proc., vol. 54, no. 7, pp. 2833-2834, July 2006.

Bonuccelli, M.A., Giunta, G., Lonetti, F., Martelli, F., "Real-time video transmission in vehicular networks", in Proc. of IEEE Int. Conf. on Mobile Networking for Vehicular Environments, pp. 115-120, 2007.

Campisi, P., Carli, M., Giunta, G., Neri, A., "Tracing watermarking for multimedia communication quality assessment", in Prioc. of IEEE Int. Conf. on Commun. ICC 2002. Vol. 2, pp. 1154-1158, 2002.

Chen, I-T., Yeh, Y.-S., "Security analysis of transformed-key asymmetric watermarking system", IEEE Signal Processing Letters, vol. 13, no. 4, pp. 213-215, April 2006.

Choi, H., Lee, K., Kim, T., "Transformed-key asymmetric watermarking system", IEEE Signal Processing Letters, vol. 11, no. 2, part 2, pp. 251-254, Feb. 2004.

Fu, Y. G., "Asymmetric Watermarking Scheme Based on Shuffling", Procedia Engineering, Volume.29, pp.1640, 2012.

Furon, T., Duhamel, P., "An Asymmetric Watermarking Method", IEEE Trans. on Signal Proc., vol. 51, no. 4, pp. 981-995, Apr. 2003.

Gui, G. F., Jiang, L.-G., Chen, H., "Linear transformation-based asymmetric watermarking scheme", Journal of Electronic Imaging, Volume.15, Issue.3, pp.033012, 2006a.

Gui, G. F., Jiang, L.-G., Chen, H., "A new asymmetric watermarking scheme based on a real fractional DCT-I transform", Journal of Zhejiang University SCIENCE A, Volume.7, Issue.3, pp.285, 2006b.

Mi He, Lizhi Cheng, "Asymmetric Watermarking Method Based on Subspace Projection", The 9th International Conference for Young Computer Scientists, 2008. ICYCS 2008., pp. 1446 – 1452, 2008.

Jun, K. X., Jun, D. L., "A Digital Watermarking Algorithm Based on Image Segmentation and DFT", 1st International Conference on Information Science and Engineering (ICISE), pp. 1511 – 1514, 2009.

Jun, W., Wei, Z., Mi, Z-K., Xie, J-Y., "A FDCT-based Asymmetric Watermarking Scheme", Second International Conference on Communications and Networking in China, 2007. CHINACOM '07., pp. 351 – 354, 2007.

Li, Y., Wei, C.-H., "Digital Image Authentication : A Review", International Journal of Digital Library Systems, Volume.2, Issue.2, pp.55, 2011, ISSN: 19479077,

Tzeng, J., Hwang, W.-L., Chern, I-L., "An Asymmetric Subspace Watermarking Method for Copyright Protection", IEEE Trans. on Signal Proc., vol. 53, no. 2, pp. 784-792, Feb. 2005.

Xie, R., Wu, K., Du, J., Li, C., "Survey of Public Key Digital Watermarking Systems", 8th ACIS Int. Conf. on Software Eng., Artificial Intell., Networking, and Parallel/Distributed Comp., vol 2, pp. 439-443, 2007.

Zhang, L., Zhou, P.-P., "Localized affine transform resistant watermarking in region-of-interest", Telecommunication Systems, Volume.44, Issue.3-4, pp.205, 2010.

Francesco Benedetto was born in Rome, Italy, in 1977. He received the Dr. Eng. Degree in electronic engineering and the Ph.D. degree in telecommunication engineering from the Third University of Rome, Italy, in May 2002 and April 2007, respectively. In 2007, he was a research fellow of the Department of Applied Electronics of the Third University of Rome. Since 2008, he has been an Assistant Professor of Telecommunications at the Third University of Rome (2008-2012, Applied Electronics Dept.; 2013-present, Economics Dept.). In particular, he has published numerous research articles on multimedia communications and video coding, ground-penetrating radar (GPR) signal processing, spread-spectrum code synchronization for 3G communication systems and satellite systems (GPS and GALILEO), correlation estimation, and spectral analysis. He has been the Session Chair at the 2012 IEEE Vehicular Technology Conference (VTC2012-Fall) for both the sessions "Detection and Estimation" and "MIMO/OFDM-based Cognitive Radio". He is the Guest Editor of the Special Issue of the Journal of Recent Patents on Computer Science on "Recent Advances in Cognitive Radio Communications". In 2012, He has been appointed as external referee (reviewer) from the Romanian Government (Ministry of Education, Research, Youth and Sport) through the National Research Council (CNCS). Since 2010, He is an Editor for the ISRN Communications and Networking, one of the International Scholarly Research Network Series of Journals of the Hindawi Publishing Corporation. Dr. F. Benedetto is a reviewer for the IEEE transactions on communications, the IEEE transactions on vehicular technology, the IEEE transactions on geoscience and remote sensing, the IEEE transactions on wireless communications, and the IEEE communications letters. He is a member of the TPC (Technical Program Committee) of the

European International Conference on Signal Processing (EUSIPCO), and he also served as a reviewer for many IEEE International Conferences.

Gaetano Giunta received the Electronic Engineering degree from the University of Pisa, Italy, and the Ph.D. degree in Information and Communication Engineering from the University of Rome La Sapienza, Italy, in 1985 and 1990, respectively. In 1986, he obtained a research grant from the Italian Research Council (CNR) of Pisa, Italy. He was also (since 1989) a Research Fellow of the Signal Processing Laboratory (LTS), Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland. In 1992, he became an Assistant Professor with the INFO-COM Department, University of Rome La Sapienza. Since 1998, he has taught Digital Signal Processing in the Third University of Rome. From 2001 to 2005, he worked in the Third University of Rome as an Associate Professor of Telecommunications. Since 2005, he has been a Full Professor of Telecommunications in the same University. He is currently the director of the Signal Processing for Telecommunications and Economics Laboratory at the Third University of Rome. His research interests include signal processing for mobile communications, video communications and security, spread-spectrum systems, satellite and wireless networks. Prof. Giunta has been a representative member of CNIT (Italian Inter-Universities Consortium for Telecommunications) and the IEEE Societies of Communications, Signal Processing, and Vehicular Technology. He has also served as a reviewer for several IEEE transactions, IET (formerly IEE) proceedings, and EURASIP journals, and a TPC member for several international conferences and symposia in the same fields.